

1 **IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

2 Application Serial No.09/507,191
3 Filing Date February 18, 2000
4 Confirmation No. 8393
5 Assignee Microsoft Corporation
6 Inventorship England, Paul
7 Group Art Unit 2136
8 Examiner Colin, Carl G.
9 Attorney's Docket No. MS1-0408US
10 Title: VERIFYING THE PRESENCE OF AN ORIGINAL DATA STORAGE MEDIUM

11 **REPLY BRIEF**

12 To: Mail Stop Appeal Brief - Patent
13 Commissioner for Patents
14 P.O. Box 1450
15 Alexandria, VA 22313-1450

16 From: Richard Bucher (Tel. 509-324-9256 x 216; Fax 509-323-8979)
17 Customer No. 22801

18 Sir:

19 In response to Examiner's Answer (mailed December 11, 2006), in
20 connection with Appellant's Appeal Brief (filed October 12, 2006), a Reply Brief is
21 submitted. Favorable consideration is respectfully requested.
22
23
24
25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Status of Claims

Claims 43 and 45-62 stand rejected and are pending in the Application.

1 **Grounds of Rejection to be Reviewed on Appeal**

2 Claims 43 and 45-62 stand rejected under 35 U.S.C. §103(a) as being
3 obvious over U.S. Patent No. 6,367,019 to Ansell et al. (hereinafter "Ansell") in
4 view of U.S. Patent No. 5,745,678 to Herzberg (hereinafter "Herzberg").
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Arguments

Applicant has thoroughly addressed the Office's rejections in its Appeal Brief (filed October 12, 2006). Accordingly, Applicant will hereafter briefly address the Office's "(10) Response to Argument" portion of the Examiner's Answer:

In the first and second paragraphs of the "Response to Argument" section, the Office argues:

On page 8, second paragraph of the appellant brief, appellant argues that Ansell et al, hereafter Ansell does not disclose a computer readable medium. Appellant states, *"the Office appears to forget that the storage key 504A and its individual component keys are not retrieved "from a computer-readable media". Instead, they are integrated into the player itself, each particular storage key being unique to its corresponding player (e.g., see Abstract, Column 6 (lines 34-40)). In fact, each player's key is difficult to change, "typically requiring physical deconstruction" of the portable player. (see Column 6 (line 40))."* Examiner recognizes this specific citation in Ansell. However, Appellant misinterprets the abstract of Ansell. In the abstract, Ansell makes reference to two embodiments: the binding may be performed by software using digital signature (digest or hash) or the binding may be performed by hardware embedded in circuitry (see portions of abstract below):

"The SPT is bound to a particular storage medium by including data uniquely identifying the storage medium in a tamper-resistant form, e.g., cryptographically signed. The SPT can also be bound to the storage medium by embedding cryptographic logic circuitry, e.g., integrate circuitry, in the packaging of the storage medium."

1 In addition, the citations provided in the rejection above clearly shows that keys are
2 stored in storage medium accessible by the players. In fact, *in the original specification page 18,*
3 *lines 3-4, medium is referred to as device that can store data that is accessible by a computer.*
4 The keys in Ansell are accessible by computer systems as they can be shared or exchanged
5 between players and cryptographically signed (figure 8B, steps 818 and 868, column 10, lines
6 43-48), therefore they are not binded by hardware, but by cryptographic signature (software).
7 Appellant even admits on page 14 of the brief "Ansell's very operation depends on selecting
8 keys from the storage medium".

9
10 Applicant respectfully disagrees. First, Applicant notes that the excerpt from
11 the Abstract of Ansell that is reproduced above is directed to binding the track (SPT)
12 to a particular storage medium. However, as Applicant previously noted in its
13 Appeal Brief (filed October 12, 2006), the Office relies on the individual
14 component keys (Keys 506A1-4) of Ansell (see Columns 7 and 8) - which
15 together comprise storage key 504A - as disclosing "a plurality of blocks of data",
16 as claimed. This is confirmed by the fact that the Office relies on the forming of a
17 digest for each of these individual component keys as disclosing "generating a
18 digest value for each of the plurality of randomly retrieved blocks of data", as
19 claimed. As such, Applicant fails to see how this reproduced excerpt is relevant to
20 the Office's rejection.

21 Additionally, Applicant notes that the excerpts from Columns 7 and 8 of
22 Ansell, which the Office relies on with respect to "generating a digest value", are
23 directed to the mechanism by which external/portable players share read-only keys
24 in a secure manner. (see Ansell, Column 7 (lines 45-48)). In this regard, a second
25 external/portable player selects "the one of keys 505A, 506A1-4 whose digest is

1 accurately represented in storage key field 406.” (see Ansell, Column 8 (lines 45-
2 55)). If no digest is accurately represented, playback on the external device is
3 aborted. Thus, at best this excerpt teaches determining whether or not
4 external/portable player 150 includes the storage key used by player 110. (Id.)
5 Nothing, however, even remotely suggests “determining that the computer-
6 readable media contains an *original version* of the given content ...”, “verifying
7 whether the received plurality of blocks are from an *original version* of the given
8 content...” or “to verify whether the received plurality of blocks are from an
9 *original version* of the given content...”, as recited in independent claims 43, 50
10 and 58 respectively. As such, the Office’s reliance on Fig. 8B, which illustrates a
11 key exchange between players, is not seen to add anything of significance.

12 **In the second paragraph of the “Response to Argument” section, the**
13 **Office argues:**

14 Appellant argues on page 9, lines 2-3 of the appellant brief that
15 Ansell cannot possibly disclose *if the digest values match a subset of the verification data*.

16 Examiner respectfully disagrees. It appears that appellant is arguing the plural form of the
17 limitation in the claims. Note that figures 2 and 5 show that only one block of data is selected and
18 only if additional verification is required that another block is selected. Also the citations
19 provided by Applicant clearly shows a block is selected and a digest is performed and the result
20 is compared to the known verification data. (see for instance page 13, lines 11-17). The

21 independent claims as claimed do not require a plurality of blocks of data to be retrieved at one
22 time as argued by Applicant with respect to Ansell. . . .

23
24 Applicant respectfully disagrees and respectfully reminds the Office that
25 although the claims are interpreted in light of the specification, limitations from

1 the specification are not to be read into the claims. (See In re Van Geuns, 988 F.2d
2 1181, 26 USPQ2d 1057 (Fed. Cir. 1993)). As such, the Office's reliance on
3 various figures and excerpts from the subject specification with respect to "digest
4 values", as recited in independent claims 43, 50 and 58, appears to be misplaced.

5 **In the third paragraph of the "Response to Argument" section, the Office**
6 **argues:**

7 Appellant argues that Herzberg et al hereafter Herzberg teaches "pre-selecting sections"
8 and randomly selecting data objects from the pre-selected sections of the program. The claims
9 do not require that the data are not pre-selected. The claims merely recite "randomly retrieving
10 plurality of blocks of data" which is broader than what is argued by Appellant. Herzberg,
11 column 14, lines 63-64 explicitly recites and claims "randomly selecting a plurality of sections
12 from within the program".

13 Applicant respectfully disagrees and submits that the Office is inappropriately
14 relying on what the subject claims do not recite to justify its rejection (i.e. "[t]he
15 claims do not require that the data are not pre-selected."). Accordingly, Applicant
16 maintains that the selected data objects of Herzberg cannot be equated with
17 "randomly retrieving", "randomly retrieved" or "to request a random set of blocks
18 of data", as recited in independent claims 43, 50 and 58 respectively.
19
20
21
22
23
24
25

1 In the fourth paragraph of the "Response to Argument" section, the
2 Office argues:

3 Appellant's showing of improper motivation on page 14, second paragraph of the brief is
4 not logical. Appellant mentions that if Ansell's data blocks were retrieved randomly as
5 suggested by the Office, the keys would rarely if ever be available to form digests. Ansell
6 discloses, however, that the keys are provided to the player, therefore they would be available
7 and discloses forming a digest for each one of the keys.

8 "player logic 502A forms respective digests of each component
9 key of read-only key 504A and each of keys 506A1-4 using the
10 same algorithm employed by player 110 (FIG. 1) in step 606 (FIG.
11 6)" (column 8, lines 46-48).

12 Randomly retrieving each data and forming a digest of each randomly retrieved data
13 would be more beneficial than forming a digest for all the data in the medium as disclosed in
14 Herzberg and explained in the rejection above.

15 Applicant respectfully disagrees. As noted above, the Office relies on the
16 individual component keys (Keys 506A1-4) of Ansell (see Columns 7 and 8) -
17 which together comprise storage key 504A - as disclosing "a plurality of blocks of
18 data", as claimed. This is confirmed by the fact that the Office relies on the
19 forming of a digest for each of these individual component keys as disclosing
20 "generating a digest value for each of the plurality of randomly retrieved blocks of
21 data", as claimed. Furthermore, as Applicant explained in detail in its Appeal
22 Brief (filed October 12, 2006), Ansell's very operation depends on a player
23 selecting specific key(s) from the storage media. Accordingly, if Ansell's logic
24 was modified so that data blocks were retrieved randomly, as suggested by the
25 Office, key exchange would not occur and the *appropriate* keys would rarely, if
ever, be available. For example, in its Examiner's Answer, the Office cites to
Column 13 (lines 45-47) of Ansell and argues that a key exchange between two

1 players can be conducted by using a smartcard and thus can be equated with
2 "retrieving a plurality of blocks of data from a storage medium". (see Examiner's
3 Answer, Page 3). However, as noted above, the receiving player's logic (502A in
4 Fig. 5) in such a key exchange must take deliberate steps (e.g. read SPT 116 and
5 parse its header 302) and make specific selections (e.g. select a specific key
6 according to the digest stored in the key field (406 in Fig. 4)). (see Column 8 (lines
7 6-67). Accordingly, modifying this logic to retrieve data randomly would
8 impermissibly change Ansell's principle of operation and impermissibly render it
9 unsatisfactory for its intended purpose because the very key exchange itself could
10 not be completed.

11 12 Conclusion

13 Applicant respectfully submits that all of the Office's rejections have been
14 traversed. As such, Applicant respectfully submits that all of the claims are in
15 condition for allowance.

16
17 Respectfully Submitted,

18
19
20 Dated: 2/12/2007

By: 

Richard Bucher
Lee & Hayes, PLLC
Reg. No. 57,971
(509) 324-9256 ext. 216